Redes Inalámbricas en la Industria: Comparación WirelessHART y ZigBee

Guillermo José Núñez Sánchez
Redes Locales en la Industria. Máster en Automática, Robótica y Telemática
Camino de los Descubrimientos, s/n. 41092 Sevilla
Febrero 2016
g.nun.san@gmail.com

This paper provides an introduction to the WirelessHART and ZigBee architectures to identify and detect advantages and disadvantages of both standards and get an approximation of what protocol can better respond to the needs that require applications targeting industry and process automation manufacture. It breakdowns and analyzes important characteristics of WirelessHART and ZigBee listing the strengths that come closest to industrial applications in order to identify which is the most suitable for this function. The study shows the WirelessHART standard has more advantages than ZigBee applications aimed at industry.

***Index Terms*—WirelessHART, ZigBee, Wireless Sensors Networks (WSN), industrial.**

I. Introducción

PARA el control de procesos industriales los protocolos para redes locales en la industria como Foundation Fieldbus, Profibus y HART, ya están bien establecidos en el sector y llevan décadas usando el cableado para la comunicación [1].A pesar de que el coste de instalación y el mantenimiento del cableado para estas redes son bastantes significativos, siguen dominando en las instalaciones industriales. Además, el hecho de muchos años de experiencia con estas tecnologías cableadas y procedimientos bien establecidos para su uso en este sector, hacen que tengan un gran peso en las plantas industriales. De modo que, la voluntad de sustituir estas redes con algo completamente nuevo (WSN) es relativamente bajo [2].

En los últimos años, la conciencia de sostenibilidad en el sector industrial ha aumentado de forma dramática, demandando con urgencia planificaciones eficientes de la energía y de los procesos industriales, debido al gran aumento tanto del precio de la energía como de presiones significativas indicando la escasez de recursos energéticos. Por ello, existe una continua necesidad de mejorar la productividad y seguridad, así como la de reducir los costes. Para dar respuesta a esta tendencia, es imprescindible desarrollar a bajo coste, tener alta precisión y gran flexibilidad y además desplegar plataformas que monitoricen la energía de forma distribuida y en tiempo real [3].

En este caso, las Wireless Sensors Networks (WSN) es un área clave de inversión en la industria de fabricación y automatización de procesos. Proporcionan soluciones de automatización y control que no son factibles con sistemas cableados para mejorar la producción, la eficiencia operativa y la seguridad [4]. Algunos protocolos para implementar WSN son Bluetooth, UWB, ZigBee, Wi-Fi y Wireless HART. Aunque hay varios protocolos para implementar WSN, la adopción de la tecnología inalámbrica en las industrias de automatización de procesos de fabricación ha sido lenta. Una razón importante de esto se cree que es la falta de un estándar abierto, internacional que cumpla los requisitos industriales [5]. Esto cambió en septiembre de 2007, cuando fue lanzado oficialmente WirelessHART (como parte de la especificación HART), siendo el primer estándar abierto de comunicación inalámbrica, diseñado específicamente para aplicaciones de medición y control de procesos [6].

II. Estándares de Comunicaciones para WSN

El objetivo para los ingenieros desarrolladores de WSN es ofrecer soluciones rentables de redes inalámbricas basadas en estándares que soporten bajas tasas de datos y un bajo consumo de energía. Estos protocolos se basan en el estándar IEEE 802.15.4, sobre el cual se ha escrito una gran cantidad de artículos revisados y los principales estándar de comunicación WSN se pueden clasificar en protocolos de uso general e industriales, tal como se presenta en Figura 1. Los protocolos incluidos como propósito general incluyen Bluetooth, IEEE 802.15.4 y ZigBee, mientras que WirelessHART e ISA100.11a están categorizados como protocolos de comunicación inalámbrica industrial [7].

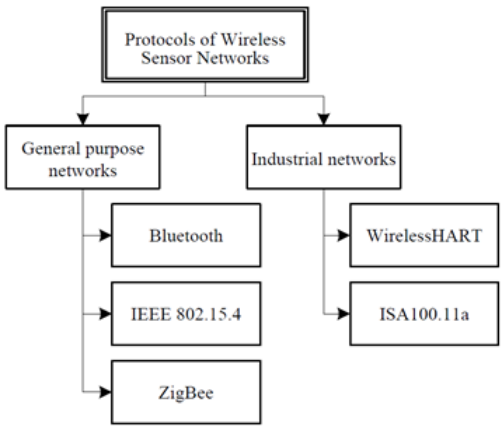

Fig. 1. Clasificación de protocolos WSN

En el transcurso del este trabajo, nos ocuparemos de describir las características más destacadas de ZigBee y Wire-

lessHART, para terminar realizando una comparación de ambos estándares indicando sus puntos fuertes y débiles respecto a aplicaciones industriales.

III. WirelessHART

WirelessHART es una extensión del protocolo HART (Highway Addressable Remote Transducer) capaz de soportar comunicaciones inalámbricas. Este protocolo nace en septiembre de 2007 [6], pero hasta 2008 no fue aprobada la especificación Wireless-HART (HART 7.1) por la International Electrotechnical Comission (IEC) como una especificación pública (IEC 62591) [8]. El estándar WirelessHART ha sido la primera tecnología de comunicaciones inalámbricas para el entorno industrial que alcanza el nivel de reconocimiento internacional [6]. Es una tecnología probada en campo con más de 100.000 dispositivos instalados en más de 8.000 redes dirigidas a aplicaciones industriales [9].

WirelessHART es una red mallada inalámbrica y está diseñado en base a una serie de requisitos fundamentales: debe ser simple (por ejemplo, fácil de usar e implementar), auto-organizable, auto-reparable y flexible (por ejemplo, soportar diferentes aplicaciones), escalable (es decir, ajustarse a las pequeñas y grandes plantas), fiable, segura y capaz de soportar la tecnología HART existente (por ejemplo, soportar comandos de HART, herramientas de configuración, etc) [10].

A. Arquitectura OSI WirelessHART

La arquitectura de WirelessHART, de acuerdo con el modelo de referencia OSI, se muestra en la Figura 2. La pila de protocolo de WirelessHART comprende cinco capas: la capa PHY que se basa en el estándar IEEE 802.15.4, la capa de Enlace (incluyendo MAC), la capa de Red, la capa de Transporte, y la capa de Aplicación [11]. Según la Figura 2, se puede observar que WirelessHART y HART son compatibles en las capas de transporte y aplicación.

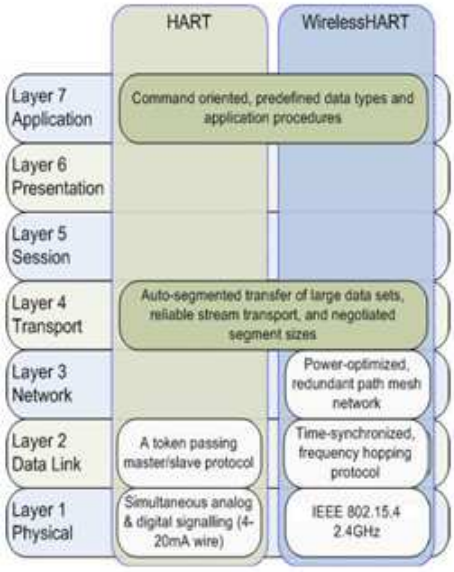
HART
WirelessHART
Layer 7 Application
Command oriented, predefined data types and application procedures
Layer 6 Presentation
Layer 5 Session
Layer 4 Transport
Auto-segmented transfer of large data sets, reliable stream transport, and negotiated segment sizes
Layer 3 Network
Power-optimized, redundant path mesh network
Layer 2 Data Link
A token passing master/slave protocol
Time-synchronized, frequency hopping protocol
Layer 1 Physical
Simultaneous analog & digital signalling (4-20mA wire)
IEEE 802.15.4 2.4GHz

Fig. 2. Torre de protocolo HART y WirelessHART.

La capa física de WirelessHART se basa principalmente en la capa física DSSS (Espectro Ensanchado por Secuencia Directa) 2.4 GHz definida en el estándar IEEE 802.15.4 [12]. Esta capa define las características de radio, tales como el método de transmisión, la potencia de la señal y la sensibilidad del dispositivo. Pues bien, así como IEE 802.15.4, WirelessHART opera en las frecuencias 2.405 – 2.4835 GHz de la banda ISM, con una velocidad de datos de hasta 250 Kbits/s, 15 canales con 5 MHz de separación entre cada canal adyacente y una potencia de hasta 10 dB [10].

La capa de enlace, es propia y opera de manera sincronizada. WirelessHART es una red basada en Acceso Múltiple por División en el Tiempo por las siglas en inglés (TDMA). Todos los dispositivos de la red están sincronizados en el tiempo y se comunica por intervalos de tiempo de longitud fija pre-programados. El uso de TDMA provee al sistema de una comunicación determinística, minimizando las colisiones y reduciendo el consumo de energía de estos dispositivos. WirelessHART también introduce el concepto Clear Channel Assessment (CCA), que es una característica opcional que permite configurar el nivel de potencia de transmisión y usar un mecanismo para no permitir el uso de ciertos canales, llamados Blacklisting (lista negra de canales), antes de transmitir un mensaje. Con CCA WirelessHART asegura de no interferir con otros sistemas inalámbricos coexistentes que tengan restricciones en tiempo real. WirelessHART coexiste en la banda compartida ISM de 2,4 GHz utilizando Frequency Hopping Spread Spectrum (FHSS) que permite a WirelessHART realizar saltos en frecuencias a través de los 16 canales definidos en el estándar IEEE 802.15.4 con el fin de evitar interferencias. Para soportar el salto de frecuencias (Channel hopping), los dispositivos WirelessHART utilizan 15 canales dentro del espectro de 2.4 GHz. El uso pseudo-aleatorio de los canales asegura que las interferencias en uno o varios canales no impidan la comunicación [10].

La capa de red y la capa de transporte, cooperan para proporcionar comunicación segura y fiable de extremo a extremo en la red. Para soportar la topología de red malla, todos los dispositivos WirelessHART deben poder reenviar paquetes en favor del resto. Hay dos mecanismos de enrutamiento definidos en WirelessHART: Graph Routing y Source Routing. En el Graph Routing, un grafo será, los múltiples caminos dirigidos que conectan a los nodos de la red. Una única red puede tener múltiples grafos, y algunos pueden solaparse. El administrador de red crea las rutas asociadas a cada grafo y las almacena en cada dispositivo de la red. Con el propósito de que si un dispositivo falla, su vecino tenga otro camino para enviar la información. Esta es la manera preferida de encaminar mensajes, tanto en el enlace ascendente como en el descendente en una red WirelessHART. El Source Routing, complementa el encaminamiento por grafo para asistir al diagnóstico de la red. Para enviar un paquete a su destino, el dispositivo fuente incluye en la cabecera una lista ordenada de los dispositivos por los cuales el paquete debe viajar [13].

La capa de aplicación, proporciona servicios de procesos de aplicación por el usuario y define los servicios necesarios de comunicación de objeto a objeto entre aplicaciones distribuidas. En WirelessHART la capa de aplicación está

orientada a comandos, y es heredada de la capa de aplicación del estándar HART para el cableado, la cual define los comandos, respuestas, tipo de datos y los reportes de estado del dispositivo[5].

B. Tipos de tramas en WirelessHART

En este punto del trabajo, se describirán las unidades de datos que se conforman en las diferentes capas del modelo OSI en WirelessHART.

En la capa física y de enlace, la unidad de datos de protocolo es la trama y tiene la siguiente forma [14] según la Figura 3:

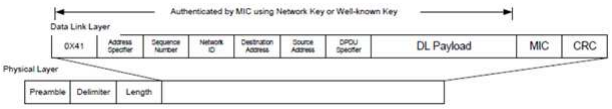

Fig. 3. Formato trama de WirelessHART.

El campo Address Specificier, se usa para especificar qué tipo de dirección es contenida en el campo origen y destino de la DPDU, ya sea un nikname de 16 bits que es asignado por el administrador de red o la dirección EUI (Identificador Único Extendido o MAC Address) de 64 bits.

En el campo DPDU Specifier los bits indica la prioridad de la DPDU.

Los 32 bits del campo MIC es un código de integridad de mensaje para la autenticación de la capa de enlace usando una clave de red. Durante el proceso de unión, el MIC del DPDU es generado usando una clave conocida (Well-Known).

Los 16 bits CRC son usados para verificar errores aleatorios para que el formato de cabecera de la capa física sea acorde al estándar IEEE 802.15.4.

En la capa de red, se muestra el único tipo de cabecera en WirelessHART, según la Figura 4, con direccionamiento y encaminamiento básico. Los campos especificaciones y parámetros de implementación de seguridad están contenidos en la subcabecera NL PayLoad [14].

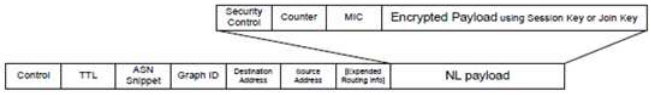

Fig. 4. Formato NPDU de WirelessHART.

En la capa de transporte, la TPDU está especificada [14] de forma simple según la Figura 5.

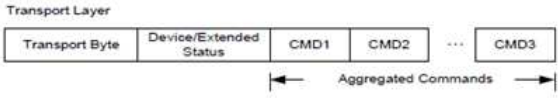

Fig. 5. Formato TPDU de WirelessHART.

El campo Transport Byte especifica el tipo de transacción (conocida o desconocida), el tipo de mensaje (petición o respuesta), la identificación del propietario de la difusión y el número de secuencia utilizado para gestionar el tráfico de paquetes.

Device/Extended status se especifica en [15].

Con el campo Aggregated Commands, WirelessHART puede transportar múltiples comandos en una simple transacción.

En la capa de aplicación, la APDU en WirelessHART puede verse como simple o con comandos agregados, donde cada uno incluye un número de comandos de 16 bits, longitud y campo de datos [14]. Se puede observar en la Figura 6.

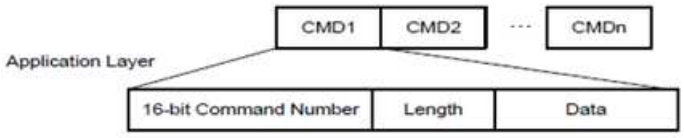

Fig. 6. Formato APDU de WirelessHART.

C. Topología de red en WirelessHART

Normalmente WirelessHART tiene una topología de red en malla, donde todos los dispositivos deben tener la capacidad de enrutamiento, es decir, pueden ser tratados por igual en términos de capacidad de red, instalación, formación y expansión, lo que amplía el alcance de la red y proporciona rutas de comunicación redundantes para aumentar la fiabilidad. Esto proporciona rutas redundantes que permite que los mensajes sean encaminados evitando obstáculos físicos, enlaces rotos e interferencias.

Por otra parte, en WirelessHART existen otras configuraciones que no son red en malla. También se puede confeccionar otras topologías de red como en árbol o en estrella como aparecen en la Figura 7, pero no son recomendadas [11].

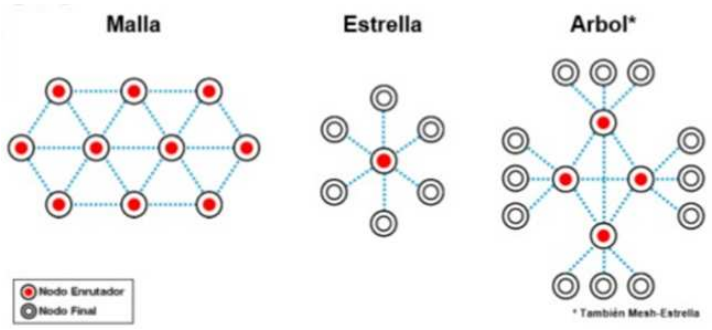

Fig. 7. Topologías de red en WirelessHART.

D. Dispositivos de una WirelessHART

La mayoría de los dispositivos en una red WirelessHART, son dispositivos de campo que se caracterizan por estar conectado directamente al proceso de una planta industrial, como pueden ser actuadores y sensores [11].

La Figura 8 muestra los diferentes tipos de dispositivos de red que comprender una red WirelessHART.

• Gateway o pasarela: actúa como interfaz entre la red WirelessHART y la planta automatizada (host). Proporciona al host acceso a los dispositivos de la red WirelessHART, y si

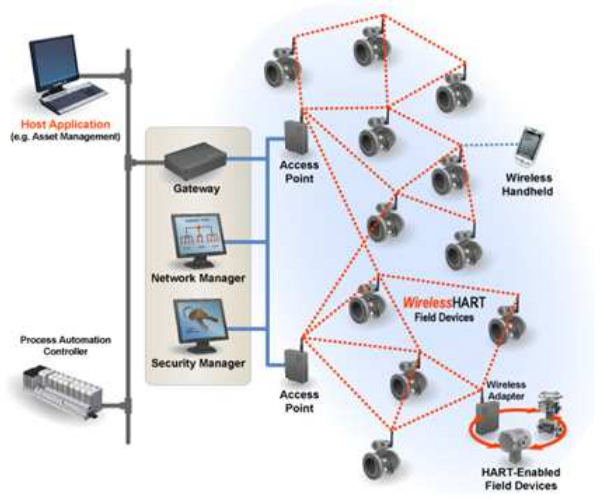

Fig. 8. Componentes de WirelessHART.

es necesario, hacer de traductor entre los diferentes protocolos [16].

• Network Manager: es el "cerebro" de la red WirelessHART. Su responsabilidad es gestionar todo lo relacionado con la red inalámbrica, como por ejemplo, la formación de la red, reconfiguración, configuración de ruta de red, gestionar la distribución de tiempos de acceso, programación de la comunicación de cada dispositivo en la red, etc. Solamente un Network Manager puede estar activo en una red WirelessHART, con la posibilidad de tener otro de backup por si el que está activo falla [16].

• Security Manager: distribuye las claves de cifrado de seguridad y mantiene la lista de dispositivos autorizados a unirse a la red [16].

• Repeater: encargados de dirigir los mensajes WirelessHART sin ningún tipo de acceso a los procesos, con el objetivo de ampliar el alcance de la red o evitar obstáculos. Todos los instrumentos en una red WirelessHART tienen la capacidad de enrutamiento [16].

• Handheld devices: se utilizan para la instalación, configuración, monitoreo y mantenimiento de todos los tipos de dispositivos WirelessHART [16].

• Adapter: unen dispositivos HART cableados a la red WirelessHART en malla [16].

• Terminal: se utiliza para unir un nuevo instrumento a una red WirelessHART existente. El terminal tiene una conexión con la puerta de enlace y, después, a un instrumento que puede ser utilizado para el diagnóstico [16].

• Field devices: son dispositivos de campo que se caracterizan por estar conectado directamente al proceso de una planta industrial y tener capacidades de enrutamiento de paquetes en la red de malla [16].

E. Seguridad en WirelessHART

En WirelessHART la seguridad es obligatoria, no hay opción para desactivarla completamente. WirelessHART aplica protección de seguridad a través de encriptación de carga útil (payload) y autenticación de mensajes para mensajes de salto simple (hop-by-hop) y mensajes de extremo a extremo (end-to-end). La protección de salto simple toma lugar en la capa de enlace de datos, mientras que la protección de mensajes extremo a extremo es llevada a cabo por la capa de red de WirelessHART. Mientras que la seguridad en la capa de red y transporte protege de posibles ataques en las rutas de la red entre el transmisor y el receptor, la seguridad en la capa de enlace de datos defiende de posibles ataques desde fuera del sistema.

WirelessHART soporta contadores con modos de operación para proveer seguridad a la información, confidencialidad y autenticidad como el cipher block chaining message authentication code (CCM) [12] en conjunto con el Estándar de Encriptación Avanzada (AES) 128 (Estandar con un bloque de tamaño de 128 bits) cifra bloques usando claves simétricas para la encriptación y autenticación de mensajes [5].

En WirelessHART se define un grupo de claves de seguridad. Los dispositivos nuevos que se quieren unir a la red deben conocer la clave de acceso a la red antes de unirse a esta. Por otra parte, adicionalmente a la clave de sesión es usada por la capa de red para la autenticación de comunicaciones extremo a extremo entre dos dispositivos y es diferente por cada par de comunicaciones. La clave de red es usada por la capa de enlace de datos para autentificar mensajes en base a un salto (one-hop). La clave y administración de la clave es responsabilidad del Security Manager y distribuida a los Field Devices por el Network Manager.

IV. ZigBee

El nombre de "ZigBee" ha sido tomado de las abejas domésticas, que emplean un patrón en zigzag para comunicarse sobre de la ubicación del néctar. El mismo zigzag es emulado por este protocolo. ZigBee cubre las capas de red y de aplicaciones por encima del estándar IEEE 802.15.4. ZigBee fue diseñado por el grupo ZigBee Alliance que está constituido por 175 empresas. Algunos nombres conocidos que lo promueven son Chipron, Ember, Freescale, Honeywell, Mitsubishi, Motorola, Philips y Samsung. Conecta cerca de 65.000 dispositivos en redes de fácil uso. El estándar ZigBee se ejecuta en dispositivos ZigBee y pretende que sea la tecnología inalámbrica más simple y menos cara que otras WPAN. La interoperabilidad de los productos, la independencia del proveedor hace que sea un estándar preferente sobre otras soluciones patentadas.

El bajo coste permite que la tecnología sea ampliamente usada en aplicaciones de control y monitoreo inalámbrico. Sobre las bandas 868 MHz (Europa) ofrece un canal, 10 sobre la banda estadounidense 902-928 MHz y 6 canales en la banda mundial ISM 2.4 GHz. Una característica es que dispone de una garantía muy baja de Quality-of-Service, no soporta de determinismo y no emplea saltos de frecuencia haciendo susceptible a interferencias [17], [18], [19].

A. Arquitectura OSI ZigBee

La torre de protocolo ZigBee consiste en cuatro capas, como se representa en la Figura 9. La capa física y la capa de control de acceso al medio se definen en el estándar IEEE 802.15.4

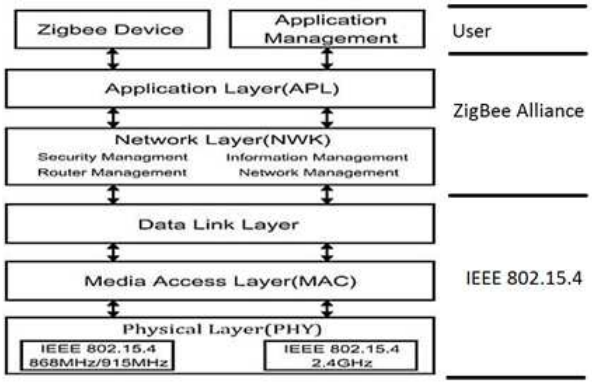

Fig. 9. Torre de protocolo ZigBee.

[12], la capa de red y la capa de aplicación están definidas por ZigBee Alliance [20].

La capa física en ZigBee se basa principalmente en la capa física DSSS (Espectro Ensanchado por Secuencia Directa) a 2.4 GHz definida en el estándar IEEE 802.15.4. Esta capa es responsable de la transmisión de datos y la gestión de canal físico [12].

La capa de enlace de ZigBee viene definida en el estándar IEEE 802.15.4. Tiene como funciones principales proporcionar enlaces de comunicaciones fiables entre entidades MAC, además de ser responsable de la creación de redes, de detectar y evitar colisiones haciendo uso de CSMA/CA [12].

La capa de red es el núcleo de ZigBee. Actúa como un puente entre la capa de aplicación y la capa de enlace para los datos ZigBee, lo que garantiza la seguridad y la creación de redes. En esta capa se aplican mecanismos que permite que los nodos se unan o salgan de la red. Se aceptan o rechazan otros nodos externos a la red. Además existen otros mecanismos para descubrir y mantener rutas [19].

La capa de aplicación es la capa más alta definida por la especificación y es la interfaz entre el sistema de ZigBee y los usuarios. Soporta aplicaciones que realizan servicios para los end points y ZigBee device objects. Sus componentes principales son:

Application Framework. Proporciona un entorno en el que las aplicaciones se ejecutan.

ZigBee Device Object (ZDO). Responsable de definir el rol del dispositivo.

Application Support Sub-layer. La interfaz entre la capa de red y la capa de aplicación [19], [21].

B. Tipos de tramas en ZigBee

En este punto del trabajo, se describirán las unidades de datos que se conforman en las diferentes capas del modelo OSI en ZigBee.

En la capa física la unidad de datos de protocolo tiene la siguiente forma [12] según la Figura 10:

El campo Preámbulo tiene 32 bits que se utilizan para sincronización de símbolos.

El campo Delimitador formado por 8 bits que se utilizan para sincronizar la recepción del frame.

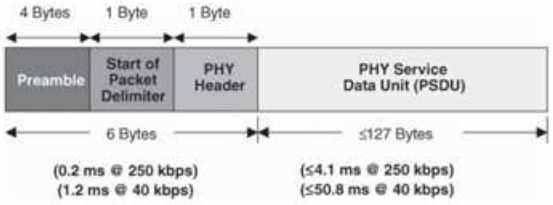

Fig. 10. Estructura del paquete de capa física IEEE 802.15.4.

El campo Cabecera comprende 8 bits que especifican la longitud de la unidad de datos (PSDU, PHY Service Data Unit).

El campo Datos puede contener hasta 127 bytes de datos.

En la capa de enlace ZigBee utiliza el estándar IEEE 802.15.4. El empaquetamiento en esta capa se realiza en cuatro tipos diferentes de paquetes, los cuales son: baliza, MAC, ACK y datos. En la Figura 11 [12] se muestran los campos de los cuatro tipos de tramas:

Trama de balizados para transmisión de balizas (Beacon frames).

Trama de datos.

Trama de asentimiento para confirmar la recepción (Acknowledgement frames).

Trama de comandos MAC.

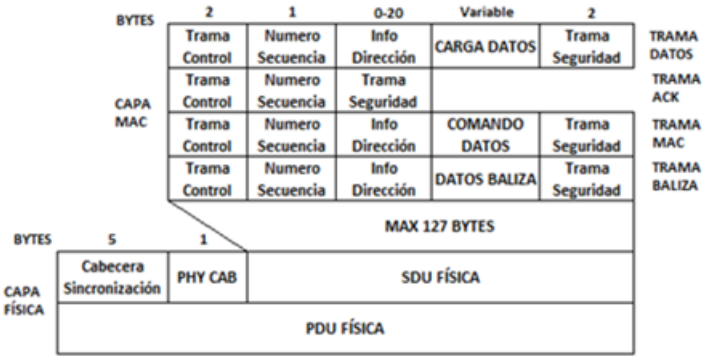

Fig. 11. Estructura del paquete de capa física IEEE 802.15.4

En la capa de red, se muestra el formato de paquete que se conforma en ZigBee según la Figura 12 [18].

Octets: 2	2	2	1	1	0/8	0/8	0/1	Variable	Variable
Frame control	Destination address	Source address	Radius	Sequence number	Destination IEEE Address	Source IEEE Address	Multicast control	Source route subframe	Frame payload
NWK Header									Payload

Fig. 12. Formato general NPDU de ZigBee.

NWK header: se encarga del control, direccionamiento e información de secuencia.

NWK payload: indica longitud variable. Contiene información específica sobre el tipo de trama.

En la capa de aplicación, la APDU en ZigBee puede verse en la Figura 13 [18].

Octets:	1	0/1	0/2	0/2	0/2	0/1	1	0/ Variable	Variable
	Frame control	Destination endpoint	Group address	Cluster identifier	Profile identifier	Source endpoint	APS counter	Extended header	Frame payload
		Addressing fields							
	APS header								APS payload

Fig. 13. Formato APDU de ZigBee.

APS header: contiene información de control y direccionamiento.

APS payload: de longitud variable. Contiene información específica sobre el tipo de trama.

C. Topología de red en ZigBee

ZigBee soporta tres tipos de topologías diferentes: peer-to-peer, estrella y cluster-árbol, según la Figura 14.

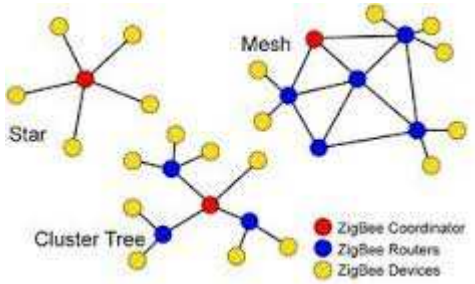

Fig. 14. Topología y componentes de una red ZigBee

En la topología de estrella, la comunicación entre los end devices se hace siempre a través del coordinator.

En la topología peer-to-peer (malla), en diferencia con la topología en estrella cada dispositivo puede comunicarse con cualquier otro dispositivo. Una red en malla, puede ser ad hoc y auto-organizarse.

La red cluster-árbol es un caso especial de una red en malla. Hay un coordinator. Un router ZigBee con sus end devices asociados. La comunicación entre end devices se hace siempre a través del router [22].

D. Dispositivos de una red ZigBee

En el estándar ZigBee hay dos clases de dispositivos de red tal como el Full-Function Devices (FFD) y el Reduced Function Devices (RFD). Los dispositivos FFD pueden realizar las funciones de coordinator o router y los dispositivos RFD solo pueden funcionar como end devices. Por otra parte, los FFD pueden formar redes de cualquier tipo, ya sea en malla, estrella, híbridas; mientras que los RFD solo se pueden conectar a un nodo con función completa [19].

Una red ZigBee está compuesta por los siguientes componentes. Figura 14:

• Coordinator - Este dispositivo inicia y controla la red. El coordinador almacena información acerca de la red, lo que incluye actuar como un centro de confianza y de ser el depositario de claves de seguridad [19].

• Router - Estos dispositivos extienden la cobertura de área de la red, proporcionan rutas de respaldo en caso de congestión en la red o de fallo de dispositivo. Pueden conectarse al coordinador y otros routers, y también conecta end devices [19].

• End Devices - Estos dispositivos pueden transmitir o recibir mensajes, pero no pueden realizar ninguna operación de enrutamiento. Deberán estar conectados ya sea al coordinador o a un router [19].

E. Seguridad en ZigBee

En Zigbee la seguridad no es obligatoria. Sin embargo, mecanismos para la autenticación, integridad y cifrado están presentes tanto en la capa de red como para la capa aplicación. En la capa MAC la seguridad está disponible a través del estándar 802.15.4, no se aborda explícitamente en el estándar ZigBee, y su uso podría romper la interoperabilidad entre diferentes productos de los proveedores. ZigBee hace uso de los mecanismos de seguridad contenidos en el estándar 802.15.4; es decir, usa contadores como el CBC-MAC en conjunto con encriptación AES-128, pero con única opción de emplear sólo encriptación o sólo integridad. Se usan tres tipos de claves: Master key, Link key y Network key. La master key es comparable a la clave de acceso en WirelessHART y es necesario para unirse a la red. La Link key se utiliza para la encriptación de extremo a extremo y tendría que ser proporcionada por el más alto nivel de seguridad a costa de más requerimientos de almacenamiento. La network key es compartida entre todos los dispositivos, y por lo tanto presenta un menor nivel de seguridad, aunque con el beneficio de que se necesita menos requerimientos de almacenamiento en los dispositivos. Todas las claves se pueden establecer desde fábrica, o ser distribuidas desde el coordinador de la red o coordinator, ya sea a través del aire (OTA), o por medio de una interfaz física. Para aplicaciones de ámbito comercial, el coordinador puede controlar la unión de nuevos dispositivos a la red y actualizar periódicamente la clave de red (Network key) [11].

V. Comparación

A la hora de realizar una comparación entre los estándares ZigBee y WirelessHART se encuentran las siguientes diferencias:

En primer lugar, en Zigbee no hay diversidad de frecuencia ya que toda la red comparte el mismo canal estático, provocando que sea altamente susceptible tanto a las interferencias intencionadas como a las no intencionadas. Esto significa que puede sufrir un grave desvanecimiento selectivo en frecuencia, debido a que los entornos de propagación en plantas industriales abundan metales, por lo que puede parar toda la comunicación ZigBee. Por otra parte, el canal estático también aumentará las interferencias con otros sistemas WLAN, y aumentará los retardos; y al mismo tiempo que el tamaño de la red aumenta, irán aumentando las colisiones y por tanto se forzarán las retransmisiones. En cuanto a WirelessHART, los saltos y la distribución de la frecuencia limita los efectos de interferencia temporal y en frecuencia (una retransmisión se producirá en una frecuencia diferente). También limita la interferencia que WirelessHART provocaría en otras redes.

En segundo lugar, no hay diversidad en rutas de encaminamiento lo que significa que en el caso de que un enlace se caiga, hay que configurar una nueva ruta desde el origen al destino. Esto aumentará los retrasos, y el modo route-discovery consumirá eventualmente todo el ancho de banda disponible en entornos con rutas inestables. Esta falta de robustez hará que ZigBee sea menos adecuado para aplicaciones de control. Sin embargo, en WirelessHART la configuración de red en malla con encaminamiento gráfico, proporciona redundancia de rutas y por tanto la propiedad de auto-recuperación reducirá notablemente los enlaces caídos. La robustez de WirelessHART abre la posibilidad para el control de manera inalámbrica, al menos para procesos lentos y no críticos.

Al usarse en ZigBee el mecanismo de acceso al medio CSMA / CA hace que los end devices estén activo demasiado tiempo por lo que el uso de baterías es inadecuado. Por otra parte, el uso de TDMA y los intervalos de tiempo preprogramados evitan colisiones de mensajes y permite que los dispositivos ahorren energía debido a que los dispositivos sólo necesitarán mantenerse activos durante los intervalos de tiempo requeridos. El gran coste que introduce WirelessHART es usar TDMA como acceso al medio, ya que se requiere de una gran sincronización; pero, en WirelessHART la información de tiempo no requiere del tráfico de la red de forma adicional, sino que ya está incrustado en el tráfico relacionado con la automatización de procesos.

La seguridad en ZigBee puede en gran medida ser configurado para cumplir los requisitos de los usuarios en la industria, aunque se debe tener cuidado al usar equipo de proveedores que no soportan los mecanismos de seguridad necesarios. WirelessHART es un protocolo seguro y proporciona varias capas de protección. Todo el tráfico está garantizado; la carga útil está cifrada y todos los mensajes se autentican, tanto en un single-hop, como en un end-to-end. WirelessHART requiere que todos los dispositivos estén provisionado con una clave secreta de acceso así como de un identificador de red con el fin de unirse a la red.

La Tabla 1 resume lo expuesto en este apartado:

TABLE I
ANÁLISIS COMPARATIVO DE ZIGBEE Y WIRELESSHART.

Características	ZigBee	WirelessHART
Capa física	IEEE 802.15.4	IEEE 802.15.4 (Protocolo Comunicación HART)
Topología	MESH, STAR, CLUSTER-TREE	MESH
Ancho de Banda	868/915 MHz y 2.4 GHz Banda ISM	2.4 GHz
Robustez	BAJA	ALTA
Seguridad	BAJA	ALTA
Latencia	ALTA	BAJA
Consumo energético	ALTO	BAJO
Coexistencia	BAJA	ALTA
Nivel de enlace	Tiene 2 capas PHY y MAC	Basada sobre la capa PHY
Encaminamiento	Enrutamiento AODV (Dispositivos descubren rutas)	Enrutamiento Gráfico (uso de rutas predeterminadas), Enrutamiento Fuente (se crea ad hoc)
Dispositivos empleados	RFD y FFD	Field Devices, Router, Adapter, Handheld, Gateway, etc

VI. CONCLUSIÓN

Al describir las características más importantes de los estándares Zigbee y WirelessHART, se realiza una comparación de ambos para saber cuál de ellos es más acertado en aplicaciones industriales.

La comparación muestra que WirelessHART aborda muchas de las debilidades de ZigBee, siendo más adecuado para dichas aplicaciones en la industria. Esto se debe a que WirelessHART fue diseñado para abordar algunas de las principales preocupaciones planteadas por la industria en cuanto al uso de ZigBee. Está diseñado desde un principio para ser un protocolo de comunicaciones robusto y seguro. Por lo que tiene más éxito que ZigBee si se implanta en aplicaciones industriales. Aunque se describen las características más importantes de ambos estándares como infraestructura, no se especifica cómo debe llevarse a cabo otras funcionalidades como la gestión de la red. Es decir, la forma en que debe hacerse es una cuestión abierta. Esto ofrecería muchas oportunidades para crear soluciones optimizadas y mejoradas.

REFERENCES

[1] G. Huang, D. Akopian, and C. P. Chen, "Measurement and characterization of channel delays for broadband power line communications," *Instrumentation and Measurement, IEEE Transactions on*, vol. 63, no. 11, pp. 2583–2590, 2014.

[2] M. Nixon and T. Round Rock, "A comparison of wirelesshartŹ and isa100. 11a," *Whitepaper, Emerson Process Management*, 2012.

[3] X. Lu, S. Wang, W. Li, P. Jiang, and C. Zhang, "Development of a wsn based real time energy monitoring platform for industrial applications," in *Computer Supported Cooperative Work in Design (CSCWD), 2015 IEEE 19th International Conference on*. IEEE, 2015, pp. 337–342.

[4] P. Radmand, A. Talevski, S. Petersen, and S. Carlsen, "Comparison of industrial wsn standards," in *2010 4th IEEE International Conference on Digital Ecosystems and Technologies (DEST), IEEE, Dubai, United Arab Emirates*, 2010, pp. 632–637.

[5] S. Petersen and S. Carlsen, "Wirelesshart versus isa100. 11a: the format war hits the factory floor," *Industrial Electronics Magazine, IEEE*, vol. 5, no. 4, pp. 23–34, 2011.

[6] J. Song, S. Han, A. K. Mok, D. Chen, M. Lucas, and M. Nixon, "Wirelesshart: Applying wireless technology in real-time industrial process control," in *Real-Time and Embedded Technology and Applications Symposium, 2008. RTAS'08. IEEE*. IEEE, 2008, pp. 377–386.

[7] T. Alhmiedat, "A survey on environmental monitoring systems using wireless sensor networks," *Journal of Networks*, vol. 10, no. 11, pp. 606–615, 2016.

[8] I. Comission, "Iec 62591: Industrial communication networks–wireless communication network and communication profiles–wirelesshart," 2009.

[9] T. D. Chung, R. B. Ibrahim, V. S. Asirvadam, N. B. Saad, and S. M. Hassan, "Adopting ewma filter on a fast sampling wired link contention in wirelesshart control system."

[10] H. website. (2010) Wirelesshart overview, tipo @ONLINE. [Online]. Available: http://en.hartcomm.org/hcp/tech/wihart/wireless_overview.html

[11] T. Lennvall, S. Svensson, and F. Hekland, "A comparison of wirelesshart and zigbee for industrial applications," in *IEEE International Workshop on Factory Communication Systems*, vol. 2008, 2008, pp. 85–88.

[12] I. . W. Group *et al.*, "Ieee standard for local and metropolitan area networksŮpart 15.4: Low-rate wireless personal area networks (lr-wpans)," *IEEE Std*, vol. 802, pp. 4–2011, 2011.

[13] M. Nobre, I. Silva, and L. A. Guedes, "Performance evaluation of wirelesshart networks using a new network simulator 3 module," *Computers & Electrical Engineering*, vol. 41, pp. 325–341, 2015.

[14] G. Wang, "Comparison and evaluation of industrial wireless sensor network standards isa100. 11a and wirelesshart," 2011.

[15] W. D. S. HCF, "Hcf_spec-290, revision 1.1," *HART Communication Foundation*, 2009.

[16] H. website. (2010) Wirelesshart how it works, tipo @ONLINE. [Online]. Available: http://sp.hartcomm.org/protocol/wihart/wireless_how_it_works.html

[17] W. Ikram and N. F. Thornhill, "Wireless communication in process automation: a survey of opportunities, requirements, concerns and challenges," in *Control 2010, UKACC International Conference on*. IET, 2010, pp. 1–6.

[18] Z. Alliance *et al.*, "Zigbee specification," 2006.

[19] V. Jindal and A. Verma, "The underlying technologies in wsns: Zigbee vs. wireless hart," in *Fuzzy Systems and Knowledge Discovery (FSKD), 2015 12th International Conference on*. IEEE, 2015, pp. 2208–2213.

[20] S. Iben Jellal, O. Cohin, S. Baranowski, U. Biaou, M. Bocquet, and A. Rivenq, "Experimental analysis of zigbee rf signal performance for railway application: Study on a laboratory reduced scale train," in *Advanced Logistics and Transport (ICALT), 2015 4th International Conference on*. IEEE, 2015, pp. 287–292.

[21] D. Gustafsson, "Wirelesshart-implementation and evaluation on wireless sensors," *Masters's Degree Project, KTH University, Electrical Engineering, Apr*, vol. 1, 2009.

[22] G. Habib, N. Haddad, and R. El Khoury, "Case study: Wirelesshart vs zigbee network," in *Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE), 2015 Third International Conference on*. IEEE, 2015, pp. 135–138.